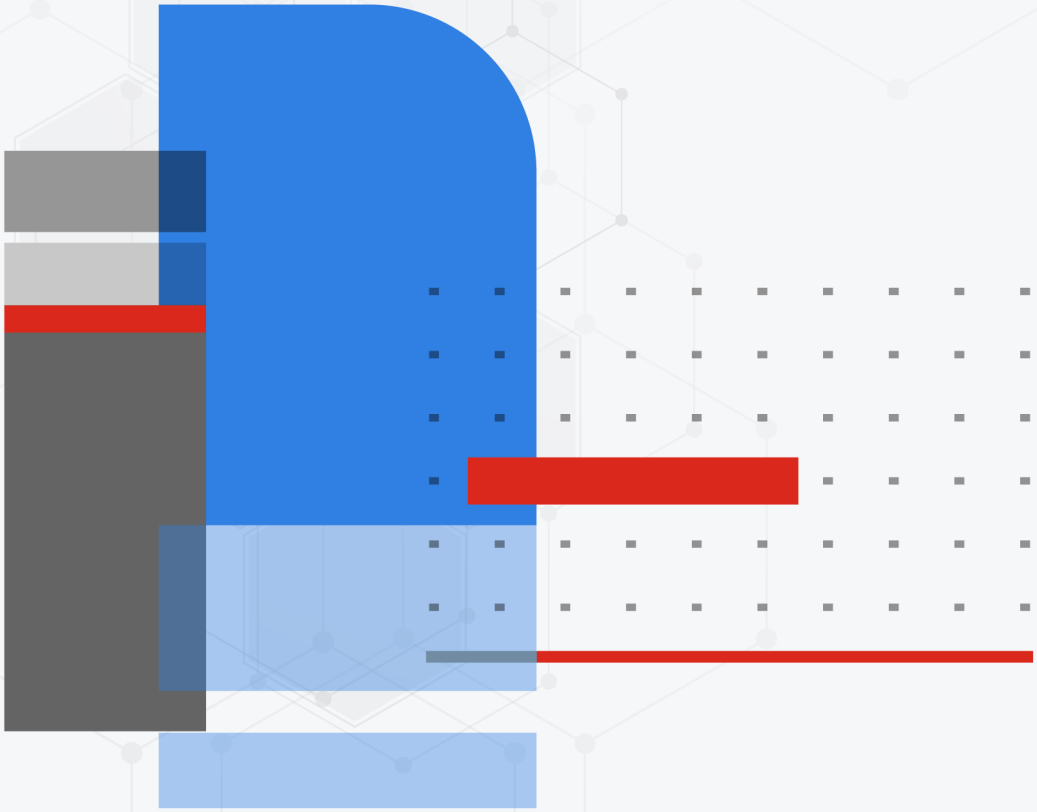
Release Notes

FortiAP-W2 7.2.2



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

April 19, 2023
FortiAP-W2 7.2.2 Release Notes
40-722-886114-20230419

TABLE OF CONTENTS

Change log

Date	Change description
2023-02-28	Initial release.
2023-04-19	Added Common vulnerabilities and exposures on page 9.

Introduction

This document provides release information for FortiAP-W2 version 7.2.2, build 0317:

For more information about your FortiAP device, see the *FortiWiFi and FortiAP Configuration Guide*.

Supported models

FortiAP-W2 version 7.2.2, build 0317 supports the following models:

Models
FAP-221E, FAP-222E, FAP-223E, FAP-224E, FAP-231E

FortiAP-W2 models do not have the unified threat management (UTM) functionality.

New features or enhancements

The following table includes FortiAP-W2 version 7.2.2 new features and enhancements:

Bug ID	Description
831005	Report to FortiGate WiFi Controller the information of wired clients on the LAN port that is bridged to a tunnel-mode SSID. The LAN port is applicable in either case: • LAN port of FortiAP model(s) with LAN and WAN ports; • LAN2 port of FortiAP model(s) with LAN1 and LAN2 ports (when WAN-LAN mode is configured on both the FortiGate and the FortiAP). Details about wired clients are displayed in: • the FortiGate CLI using "`diagnose wireless-controller wlac -c lan-sta`" and • the FortiAP CLI using "`cw_diag -c k-lan-host`".

Upgrade and downgrade information

Upgrading to FortiAP-W2 version 7.2.2

FortiAP-W2 version 7.2.2 supports upgrading from FortiAP-W2 version 7.0.3 and later.

Downgrading to previous firmware versions

FortiAP-W2 version 7.2.2 supports downgrading to FortiAP-W2 version 7.0.3 and later.

Firmware image checksums

To get the MD5 checksum code for a Fortinet firmware image, perform the following steps:

1. Go to the Fortinet Support website.
2. Log in to your account. If you do not have an account, create one and then log in.
3. From the top banner, select **Download > Firmware Image Checksums**.
4. Enter the image file name, including the extension. For example, FAP_S221E-v600-build0233-FORTINET.out.
5. Click **Get Checksum Code**.

Supported upgrade paths

To view all previous FortiAP-W2 versions, build numbers, and their supported upgrade paths, see the Fortinet Documentation website.

Product integration and support

The following table lists product integration and support information for FortiAP-W2 version 7.2.2:

FortiOS	7.2.4 and later
Web browsers	Microsoft Edge version 41 and later
	Mozilla Firefox version 59 and later
	Google Chrome version 65 and later
	Apple Safari version 9.1 and later (for Mac OS X)
	Other web browsers may work correctly, but Fortinet does not support them.

We recommend that the FortiAP firmware version be matched with the respective FortiOS version, when available. Other variations of FortiOS and FortiAP versions may technically work for the lowest common feature set. However, if problems arise, Fortinet Support will ask that the versions be matched, as recommended, before troubleshooting.

Resolved issues

The following issues have been resolved in FortiAP-W2 version 7.2.2. For inquiries about a particular bug, visit the Fortinet Support website.

Bug ID	Description
686411	Fixed a kernel panic issue in function call `dev_hard_start_xmit`.
741017	FortiAP received too many false "antenna defect detected" logs.
752868	Fixed a kernel panic issue `PC is at skb_recycler_alloc+0x10c/0x26c`.
767916	When wireless clients are connected to different radios of the same tunnel-mode SSID with static or dynamic VLAN, they cannot ping each other.
776536	Fixed a kernel panic issue `PC is at _ieee80211_find_node+0x4/0xac [umac]`.
829304	FortiAP didn't properly report LLDP neighbors to FortiGate WiFi Controller.
832926	FortiLAN Cloud Captive Portal didn't work with NAT mode and Deny Local LAN.
836078	Local-bridging SSID with external captive portal could not invoke MAC Authentication Bypass (MAB) on Cisco ISE, when wireless clients disconnected and then reconnected.
836216	When FortiGate WiFi Controller is running FortiOS 7.2.1 (or later), some 2.4GHz-band clients could not connect with managed FortiAP-W2 units.
859528	The priority order of multiple AC IP addresses in DHCP Offer was not honored.
868752	FortiAP with region code E cannot support country code SA (Saudi Arabia).
874299	Bluetooth functions of FAP-221E Gen3 and FAP-223E Gen3 could not work.
876071	SNMP daemon would randomly become stuck with high CPU usage.

Common vulnerabilities and exposures

FortiAP-W2 version 7.2.2 is no longer vulnerable to the following common vulnerabilities and exposures (CVE) reference:

Bug ID	Description
802993	CVE-2023-25608 (Arbitrary file read through the CLI).

For details, visit the FortiGuard Labs website.

Known issues

The following issues have been identified in FortiAP-W2 version 7.2.2. For inquiries about a particular bug or to report a bug, visit the Fortinet Support website.

Bug ID	Description
537931	FAP-222E doesn't support the FortiAP Configuration mode. Push and hold the RESET button on the POE adapter for more than 5 seconds to reset FAP-222E to the factory default.
655887	FAP-221E/223E gets low throughput on tunnel SSID when its wtp-profile has set `dtls-policy ipsec-vpn`.
692160	Wireless packets captured by FortiAP radio in Sniffer mode are corrupted.

www.fortinet.com